UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/822,069 | 04/09/2004 | Jeffrey A. Kraemer | 368605 | 2093 |

76863 7590 02/19/2009

KRAGULJAC & KALNAY
4700 ROCKSIDE ROAD
SUMMIT ONE, SUITE 510
INDEPENDENCE, OH 44131

| EXAMINER | |
|---|---|
| DOAN, TRANG T | |
| ART UNIT | PAPER NUMBER |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/19/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/822,069 | KRAEMER ET AL. | |
| | Examiner | Art Unit | |
| | TRANG DOAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,6-20,41 and 46-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,6-20,41 and 46-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to the amendment filed on 12/08/2008.

2. Claims 1 and 41 have been amended.

3. Claims 2-5, 21-40, 42-45 and 61-98 have been canceled.

4. Claims 1, 6-20, 41 and 46-60 are pending for consideration.

### *Continued Examination Under 37 CFR 1.114*

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/08/2008 has been entered.

### *Response to Arguments*

6. Applicant's arguments with respect to claims 1, 6-20, 41 and 46-60 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 6-20, 41 and 46-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter et al. (US 2003/0051026) (hereinafter Carter) in view of Rokosz (US 7092866) (hereinafter Rokosz).

Regarding claims 1 and 41, Carter discloses:

(A) defining at least one security rule specifying whether to allow or deny a request to access at least one resource under a given set of circumstances (Carter: See Abstract section and paragraphs 0168-0169, 0171, 0258, 0607 and 0802-0803: four sets of policies included in the Network Surveillance and Security System that govern access to databases (i.e., resource));

(B) supplying at least one request to access a resource (Carter: See paragraphs 0180, 0652 and 0755: A Security Reference Monitor is a hidden controller that makes references against the Security Reference Database whenever the Security Reference Monitor detects that the Security Authorization Database receives a request for access); and

(C) applying the at least one security rule in response to the at least one request to access a resource to determine whether to allow or prevent the at least one request (Carter: See paragraphs 0180, 0785 and 0797-0803: the watchdog system may use its own policies to permit or deny access, or it may pass the decision to other components of the Network Surveillance and Security System).

Carter does not explicitly disclose controlling the reference monitor simulator to operate at an accelerated rate as compared to an actual reference monitor by providing at least one parameter that defines a system environment in which the reference monitor simulator executes, where the at least one parameter includes a time parameter, where the time parameter controls one or more of, eliminating a time gap between trace requests, indicating that a time period between portions of a trace request has elapsed, and running a system clock faster than real-time. However, Rokosz discloses controlling the reference monitor simulator to operate at an accelerated rate as compared to an actual reference monitor by providing at least one parameter that defines a system environment in which the reference monitor simulator executes, where the at least one parameter includes a time parameter, where the time parameter controls one or more of, eliminating a time gap between trace requests, indicating that a time period between portions of a trace request has elapsed, and running a system clock faster than real-time (Rokosz: column 11, lines 44-61; and column 11 line 65 through column 12 line 32). Therefore, it would have been obvious to a person skilled art at the time the invention was made to have included in Carter the feature of Rokosz as discussed above because a need exists for a technique to test the performance of software which normally would take an extended period of time to observe. Another a need exists for a technique to compress the testing time for certain software, including knowledge management products, to a rate faster than one second per second (Rokosz: column 1, lines 39-44).

Regarding claims 6 and 46, Carter as modified discloses (D) assessing the effectiveness of the at least one security rule (Carter: paragraphs 0222 and 0260).

Regarding claims 7 and 47, Carter as modified discloses wherein assessing the effectiveness of the security rule further comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed (Carter: paragraphs 0260, 0606-0611 and 0802).

Regarding claims 8 and 48, Carter as modified discloses wherein assessing the effectiveness of the security rule further comprises determining a rate of improper requests prevented (Carter: paragraphs 0403 and 0411-0413).

Regarding claims 9 and 49, Carter as modified discloses wherein (B) further comprises an application program supplying the at least one request to access a resource (Carter: paragraph 0304).

Regarding claims 10 and 50, Carter as modified discloses wherein (B) further comprises capturing at least one request to access a resource before supplying the at least one request to access a resource (Carter: paragraphs 0172 and 0218).

Regarding claims 11 and 51, Carter as modified discloses wherein a reference monitor performs the capture of the at least one request to access a resource (Carter: paragraphs 0700 and 0755).

Regarding claims 12 and 52, Carter as modified discloses wherein the reference monitor which performs the capture of the at least one request to access a resource is the same type of reference monitor as the reference monitor whose operations are recreated by the reference monitor simulator (Carter: paragraphs 0168-0169, 0180, 0700 and 0755-0756).

Regarding claims 13 and 53, Carter as modified discloses wherein the captured at least one request to access a resource is an improper request (Carter: paragraphs 0180 and 0222).

Regarding claims 14 and 54, Carter as modified discloses wherein an improper request comprises a request issued by an application in response to one of a virus and a buffer overrun attack (Carter: paragraphs 0180, 0222 and 0674).

Regarding claims 15 and 55, Carter as modified discloses wherein the captured at least one request is modified prior to supplying the at least one request to access a resource (Carter: paragraphs 0700 and 0755).

Regarding claims 16 and 56, Carter as modified discloses wherein the modification is performed by a user (Carter: paragraph 0795).

Regarding claims 17 and 57, Carter as modified discloses wherein an electronic file system stores the at least one security rule, and wherein (D) further comprises the reference monitor simulator accessing the security rule in the electronic file system in response to receiving the at least one request to access a resource (Carter: paragraphs 0260, 0606-0611 and 0802).

Regarding claims 18 and 58, Carter as modified discloses wherein the at least one parameter provided to the reference monitor simulator further includes at least one of a system clock, a wrapper function, and a timer event (Carter: paragraph 0880).

Regarding claims 19 and 59, Carter as modified discloses (E) maintaining statistics on the operation of the reference monitor simulator (Carter: paragraphs 0271 and 0470).

Regarding claims 20 and 60, Carter as modified discloses wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected,

and number of requests prevented compared to number of prevented requests expected (Carter: paragraph 0470).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431